REMARKS

Applicant thanks the Examiner for the careful review of this application. Claims 1, 9, 17, 25, 32, 36, 46, 52, 56, 64, 66 and 71-76 were amended to clarify aspects of the present invention. No new matter was added. Claims 1-72 remain pending in this application.

REJECTIONS UNDER 35 U.S.C. § 102(b)

Claims 1, 5-9, 13-17, 21-25, 29-32, 46, 50-52, 60-63, 75 and 76 were rejected under 35 U.S.C. § 102(b) as being anticipated by Fiat (U.S. Patent No. 4,964,164). Applicant respectfully traverses for the following reasons.

Fiat apparently discloses a computation method for batch processing of public key encryption using a processor. The method batch processes an e1th root of a first message-data signal, M1, as $M1^{1/e1}$, and an e2th root of a second message-data signal, M2, where e1 and e2 are relatively prime, using the steps of computing an exponent product, e, by multiplying e1 times e2; computing a message product, M, wherein $M=M1^{(e/e1)}M2^{(e/e2)}$; computing a batch root, R, wherein $R=M^{1/e}$; computing the euclidean inverse, t, of e2 modulo e1; and computing $R^{e2*t}/(M1^{(e2*t-1)/e1}M2^{t})$, thereby generating $M1^{(1/e1)}$. For a plurality of message-data signals, the method batch processes a plurality of message-data-signal roots as the e1, e2, . . ., ek, roots for a plurality of message-data signals, M1, M2, . . . Mk, respectively, where the ei and ej are pairwise relatively prime for i not equal to j.

Aspects of the present invention are directed toward systems and methods for establishing a secure connection between a server and a browser such that the efficiency of completing the initial handshake process is greatly improved by batch processing four of these handshakes as opposed to processing them sequentially. Additional provisions are made to further optimize performance such as employing a scheduling algorithm that assigns certificates to incoming connections and for picking batches from pending requests.

In marked contrast, Fiat discloses batch processing of public key encryption using methods that are differently implemented than the present invention. For example, Fiat merely discloses batch processing but fails to teach that a batch of four is optimal for key sizes commonly used in SSL and other network security protection handshakes. Furthermore, Fiat's basic algorithm also does not give much improvement for these typical key sizes. Applicant further submits that Fiat's algorithms are also substantially different than those employed by aspects of the present invention.

Withdrawal of the rejections of claims 1, 5-9, 13-17, 21-25, 29-32, 46, 50-52, 60-63, 75 and 76 is respectfully requested.

REJECTIONS UNDER 35 U.S.C. § 103(a)

Claims 2, 10, 18, 26, 33, 36-37, 50-45, 53, 57, 64-67 and 70-74 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Fiat in view of Corella (U.S. Patent No. 6,763,459). Applicant respectfully traverses for the following reasons.

Fiat was previously summarized. Corella apparently discloses a public key infrastructure that includes an off-line registration authority that issues a first unsigned certificate to a subject that binds a public key of the subject to long-term identification information related to the subject and maintains a certificate database of unsigned certificates in which it stores the first unsigned certificate An on-line credentials server issues a short-term disposable certificate to the subject that binds the public key of the subject from the first unsigned certificate to the long-term identification information related to the subject from the first unsigned certificate. The credentials server maintains a table that contains entries corresponding to valid unsigned certificates stored in the certificate database. The subject presents the short-term disposable certificate to a verifier for authentication and demonstrates that the subject has knowledge of a private key corresponding to the public key in the short-term disposable certificate.

For reasons similar to those presented in the previous section, Applicant respectfully submits that Fiat, alone or in combination with Corella, does not disclose the present invention. Applicant therefore respectfully requests the withdrawal of the rejections of claims 2, 10, 18, 26, 33, 36-37, 50-45, 53, 57, 64-67 and 70-74.

CONCLUSION

Applicant believes that all pending claims are allowable and a Notice of Allowance is respectfully requested. The amendment was made to expedite the prosecution of this application. Applicant respectfully traverses the rejections of the amended claims and reserves the right to re-introduce them and claims of an equivalent scope in a continuation application.

If the Examiner believes that a conference would be of value in expediting the prosecution of this application, he is cordially invited to telephone the undersigned counsel at the number set out below.

Respectfully submitted,
PERKINS COIE LLP

J P. Kudla

Dated: March 22, 2005

Jonathan P. Kudla
Reg. No. 47,724

Customer No. 22918
Perkins Coie LLP
P.O. Box 2168
Menlo Park, CA 94026
Telephone: (650) 838-4300